U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF THE SECRETARY

DOT H 1350.252
May 22, 1999

DEPARTMENTAL GUIDE
TO
RISK ASSESSMENT
PLANNING

TABLE OF CONTENTS

DEPARTMENTAL GUIDE
TO
RISK ASSESSMENT PLANNING

1. PURPOSE

The purpose of this Guide is to provide Department of Transportation (DOT) and their Operating Administration managers, system owners, ISSO's and network administrators with a step-by-step approach for conducting risk assessments within their organizations.

2. SCOPE

The provisions of this Guide apply to the Department of Transportation (DOT), its Secretarial Offices and Operating Administrations (OA).

3. GOALS

The Goal of risk assessment planning is to provide a reasonable approach for the identification of threats, vulnerabilities and risk to DOT and OA systems and facilities. This approach will also allow for the assessment of those safeguards, which may mitigate those identified risks. This assessment will allow management to make an informed decision regarding those safeguards to be implemented and those risks to be accepted.

4. REFERENCES

The DOT Departmental Information Resources Management Manual (DIRMM) DOT H 1350.2 implements statutory and regulatory Information Resources Management (IRM) and security requirements for the Department. It also calls for ensuring the confidentiality, integrity, and availability of information contained, processed, or transmitted in/on sensitive systems. Refer to DOT H 1350.2.1 REGULATORY AND GUIDANCE DOCUMENTS for specific references.

5. OVERVIEW OF RISK ASSESSMENTS

A risk assessment is the application of a standardized methodology in the determination of threats, risk factors, vulnerability exposures and potential losses. The risk assessment is an approach to satisfying the needs of an organization to protect their assets, in which they have made a substantial investment. The risk assessment also serves the to identify the particular problems an organization could expect to encounter in the performance of its mission, and the adverse affects these problems might present to the organization's ability to meet its obligations. Finally, the risk assessment is a mechanism by which management can address these problems according to their relative importance, based on financial analysis, and develop safeguards which are both reasonable and cost-effective.

The risk assessment involves the identification or creation of a scale to measure the level of risk. This level of measurement will identify the loss of assets, degree of vulnerability, impact of threats and effectiveness of safeguards. This measurement will allow the organization to meet departmental and OA requirements, aid in the certification and accreditation process, reduce losses and protect assets.

Because risk assessments are so important to the protection of the organizations assets or the reduction of their losses, these assessments should be conducted periodically. These periods may be different, depending on some of the following factors:

- Departmental and/or OA requirements
- Departmental Policy requires that risk assessments be conducted every 3 years
- During the design and development of a new system
- Whenever there is a major change to a system

This risk assessment planning process will discuss the following major areas to ease the conduct and aid in validating the information to be collected.

- How To Approach The Assessment
  - ➢ Management Support
  - ➢ Team Composition
  - ➢ Setting The Scope
- Data Collection
  - ➢ Identifying Assets
  - ➢ Identifying Existing Controls
  - ➢ Identifying Vulnerabilities
  - ➢ Identifying Threats
- Data Analysis
  - ➢ Pairing Threats And Vulnerabilities
  - ➢ Determining Annual Loss
  - ➢ Determining Cost Effective Safeguards
- Reporting The Results

6. HOW TO APPROACH THE ASSESSMENT

A. Management Support

The key to a successful risk assessment is to have the support of management. Their support must be enlisted, and they must understand the importance of the assessment. It is critical that management's security awareness be raised. A means of accomplishing this would be to make a presentation to them, explaining the importance of conducting a risk assessment, and present them with some examples of departmental, OA or media information about current losses attributed to weak security management. Show how a risk assessment will consider the following areas:

- Mission,
- System Description,
- Assets,
- Sensitivity,
- Criticality,
- Vulnerabilities,
- Threats, and
- Safeguards.

The information obtained from this assessment will aid management in making cost effective; security-efficient decisions based on risk level acceptability. A value-added benefit of the risk assessment is that it will raise management's security awareness, --- this in the long run will assist in creating a more secure environment in which to work. However, remember that management must understand that they are a key partner in the successful completion of this activity.

In summary the key elements to obtaining management support are:

- Make a formal presentation to top level management
- Explain the importance of the risk analysis
- Use Media Examples

B. Team Composition

Once management support has been obtained, the next step to a successful risk assessment is the team composition. This team will be responsible for the collection, analysis and reporting of systems status to management. It is important in collecting information that the team encourages input from all of the security disciplines. These disciplines should include, but not be limited to:

- Physical Security,
- Personnel Security,
- Information Security (Hard Copy), and
- Automation Security (Information Technology)

Because of the complex nature of the risk assessment, the team should consist of individuals knowledgeable in each of the above areas. See Appendix A for a Sample Risk Assessment Methodology. It is normally recommended that the minimal composition of a Risk Analysis Team be 2 people. This allows for an exchange of information and ideas.

C. Setting the Scope

The goals of the risk assessment should be clear. In many systems there is the possibility that what may start out as a Local Area Network (LAN), could quickly become a Wide Area Network (WAN). Depending on the resources that have been assigned to the risk assessment task and the time constraints that have been placed on the project, the team could find themselves out of resources and time before they complete the project. It is imperative that the team and management come to an agreement in the very beginning as to what the scope is. To define the scope, the following areas should be addressed:

- Mission
- Responsibilities
- Controls
- Platforms
- Facilities
- Systems
- Applications
- LAN's / MAN's / WAN's

1) Mission –

Management must provide the team with the mission of the organization, system or application to be analyzed. This will set the baseline for the scope of the assessment. It is imperative that both management and the team are in agreement as to the baseline parameters of the assessment.

2) Responsibilities –

Management should identify points of contact for the team in the areas of physical, personnel, information, and automation security. In addition, management should provide the team with system owner, system administration and user points of contacts. The team should make initial contact to set up a general meeting to discuss the goal of the risk assessment, and identify the responsibilities of the points of contact. This will allow the team to return to management if in fact the responsibilities do not align with personnel in the areas needed to provide access to information or personnel with regards to the assessment. Once all the Points of Contact (POCs) are established, then the team, management, and the POCs should meet to identify what responsibilities are expected from the group.

3) Controls –

The team should discuss with management or their POCs to identify three critical factors:

- What controls are currently implemented,

- Their degree of implementation, and
- What controls are planned near term for implementation

This will allow the team to evaluate if the existing team composition is correct, to allow for proper evaluation of existing or planned (near term) controls. In the event that the expertise necessary to evaluate these controls does not reside on the team, the possibility does exist that the team may need to be augmented (either full or part time) to meet this need.

4) Platforms –

Identification of the platforms that are involved in the risk assessment is also critical. The risk assessment team must have an understanding of the specific platform(s) to ensure that a thorough analysis is accomplished. This again will add constraints to the proper identification and assignment of assets to the team, or in support of the team.

If an application is the target of the assessment, an additional factor that must be taken into consideration is, --- how many different platforms does that application run on? This may lead to the identification of other resources needed to accomplish the risk assessment.

5) Facilities –

The identification of facilities is key to the accomplishment of the risk assessment. No matter how secure a system is made, --- if the facility that houses it is not secure to the same or greater sensitivity/criticality level, then management is just wasting their time, assets and budget.

6) Systems –

It is critical to know the system(s) that is being analyzed, as this will also aid in determining if the assessment can be accomplished in the time allotted and with the resources assigned. In some instances, management may not be aware of the true complexities of some systems. The team should be prepared to ask management all questions necessary to determine the number of processes that a system runs, the geographical span of the system, and how the nodes on the system connect. If it appears that the system is to large geographically, then it may be prudent to advise management to look at the system on a smaller scale, possibly by region or by process. A key factor to remember is that doing a representative sampling is not normally safe, especially when looking at a system from a geographical point of view. Doing so may not take into account specific local environmental, threat or vulnerability issues.

7) Applications –

The issue of applications is partially addressed in paragraph 6) above. The team and management need to look at the applications that are run on the system. This will aid in identifying the complexity of the system, some known vulnerabilities which may affect other applications running on the system, or the system itself. Additionally, this will aid in determining the resources needed to conduct the assessment.

8) LANs/MANs/WANs –

The determination as to whether the team will be assessing a LAN, a MAN or a WAN deals with two main factors. First, --- are the resources available? Secondly, it is critical that the sensitivity of all systems that connect to or through the LAN, MAN, or WAN be identified, as it may impact the sensitivity of the LAN, MAN, or WAN as a whole.

As you can see, one of the primary reasons for defining the scope of the assessment up front is to ensure that adequate resources are assigned to the project. In addition to having the proper number of resources, the types of resources needed must also be addressed. In fact, the scoping of the assessment is the most critical pre-assessment factor. This phase of the assessment will ensure that the team understands management’s goals and desires. This will preclude any shifting of scope mid way through the assessment, and assures that the assessment is accomplished in a cost-effective manner.

D. Defining Data Collection

Data collection will involve conducting interviews, utilization of questionnaires, review of documentation and observation. This will cause the team to have to interface with many personnel involved in the securing and operations of a system or application. These personnel would include, but not be limited to:

- Users
- Operations Personnel (system administrators, help desk personnel, system technicians, etc.)
- ISSO's
- ISSM's
- Physical Security Officers
- Facility Security Officers

Documentation review would include but not be limited to:

- Access Logs
  - ➢ System
  - ➢ Maintenance
  - ➢ Visitor
- Incident Reports
- Documents
  - ➢ Plans
  - ➢ Policies
  - ➢ Procedures
- Previous Risk Assessments
- Continuity of Operations Plans
- Contingency Reports
- Directories
- Inventory Records
- Floor Plans
- Organization Charts
- Mission Statements
- System and Network Configurations

7. DATA COLLECTION

A. Identifying Assets

The first clarification that must be made is the basic definition of an asset. An asset may consist of any of the following:

- Personnel (Here include Time, Benefits, and Training.)
- Hardware
- Software
- Data (It is imperative that it's sensitivity and criticality be identified)
- Financial Systems
- Facilities
- Mission - Services

Those items listed above are not an all-inclusive listing of categories. Depending on the mission of the organization, there are things that could be added. The key here is to identify all of the assets that are associated with the system or application. One asset that is commonly overlooked when collecting asset data is personnel. Remember that systems or applications are operated and maintained by personnel, --- if access to a system or application is lost either short or long term then the cost to repair or replace the application is only a part of the true value of the loss. In addition, one would have to consider the cost of the personnel to do the repair or replacement and the loss incurred due to the number or personnel who become unproductive because of the loss of the system or application. These costs can build dramatically, depending on the system or application, and the type of loss that occurred (loss will be discussed in the paragraph below). It is important to obtain all the necessary information concerning assets associated with a system or application, as it will play a large part in the analysis phase of the risk assessment.

B. Loss Categories

Loss categories identify the type of loss that can occur to an asset, depending on the threat that is attacking it and the vulnerability that is being exploited by the threat to attack it. An explanation of these loss categories follows below.

1) Damage / Destruction

As the name implies, this loss category deals with the damage or destruction of an asset. This can occur through an act by an insider or external and can be either man made or an act of nature. To value this type of loss you would look at such items as:

- Replacement cost of the asset (Leased equipment should be treated as if it were owned),
- Time to replace the asset (obtain a new one),
- Time to setup and install the asset,
- Downtime of personnel dependant on the asset, etc.

The replacement time for data and software may involve retrieving off-site backup copies (assuming there are backups), and updating the copies to ensure that they are current.

2) Delay/Denial

Where damage/destruction looked at the replacement of assets, delay/denial looks at the loss per hour incurred by the organization. These losses could look at such items as:

- Operational cost – Cost for paying an employee during a non-productive period. A formula to calculate this cost could be:
  - ➢ Number of Employees * The Average Hourly Wage = Idle Users
- Makeup cost – Cost for paying an employee to recover from the non-productive period. This has an added incurred cost for overtime. If your system or application is unavailable for 8 hours it may take 4 hours overtime to make up for that loss.
- Loss of business or service – This can occur if another organization depends on your organization to provide it a service. This service may be obtained from another agency or organization this customer may go there for the service.

Along with the loss of delay / denial you could incur some type of “intangible loss”. This type of loss will be discussed later.

3) Disclosure

Disclosure deals with the disclosure of information. This type of loss is generally associated with data sets. This type of loss could deal with information with the following sensitivity levels:

- Official Use Only
- Privacy Act Information
- Proprietary Information
- Confidential Information
- Secret Information
- Top Secret Information
- Sensitive Compartmented Information

The Department of the Navy estimated disclosure losses as depicted in the table below.

Sensitivity Level of Data	**Disclosure Loss**
For Official Use Only	$ 1,000.00
Privacy Act or Confidential	$ 10,000.00
Secret	$ 100,000.00
Top Secret	$ 1,000,000.00

It should be noted that this loss value is per record. It is highly unlikely that every attack on a data set will result in the total disclosure of all records in the data set. Thus a factor of probably 5% would result in the actual loss value for this type of data. For example, if the data set contained 5,000 confidential records then the loss could be valued at $2,500,000 for the total loss.

4) Modification

Modification is a loss that can be intentional or unintentional. It may allow the perpetrator to obtain financial gain, skew results or destroy data. Some types of assets that could be affected by this type of loss could include, among others.

- Accounts Receivable
- Accounts Payable
- Cash Accounts
- Negotiable Instruments
- Asset Inventory

The means to value to loss incurred by this type loss would be to total all accounts with a monetary value. Since it is unlikely that all records of this nature would be modified here again a factor of probably 1% would result in the actual loss value for this type of data.

5) Intangible

Intangible losses are normally losses incurred from embarrassment and loss of credibility. These losses are very difficult to determine. One of the best ways to derive this value would be through historical losses incurred by the organization or another agency with the same type of mission. In the event that this information does not exist would be to take the total losses from all the other loss values and then use a factor of 1%.

It should be noted that this form of valuation will provide the “Worst Case” losses that could be incurred. As for most of these loss types, you will not lose the total asset. This should be identified in the final report that “Values Represented are Worst Case Losses”.

C. Identifying Vulnerabilities

A vulnerability is a weakness which a threat will exploit to attack an asset. A vulnerability can be exploited by more than one threat, and thus cause a weakness for more than one asset. It is rare that a vulnerability will only affect one asset.

One of the most effective ways to identify vulnerabilities is to develop questionnaires that address such areas as:

- Physical Security,
- Environmental,
- System Security,
- Communications Security,
- Personnel Security,
- Plans,
- Policies,
- Procedures,
- Management,
- Support, etc.

These questions should be drawn from the organization policies, plans and procedures. The purpose for this is to determine the effectiveness and degree of implementation and training that is in place, with regards to these plans policies and procedures. Once the vulnerabilities have been identified, the team should meet with management, and update them on these findings and the asset valuations. Ensure that everyone is in agreement with the findings.

D. Identifying Threats

A threat is an event, process, activity or action that exploits a vulnerability to attack an asset. The threat analysis should include such considerations as natural threats, accidental threats, human accidental threats, and human malicious threats. Threats could be such items as:

- Aircraft Accident,
- Air Conditioning Failure,
- Blackmail,
- Biological Contamination,
- Chemical Spills,
- Cold / Frost / Snow,
- Communications Loss,
- Data Destruction,
- Data Integrity Loss,
- Fire,
- Flood/Water Damage,
- Hardware Failure,
- Sabotage,
- Storms / Hurricanes,
- Substance Abuse,
- Theft of Assets or Data,
- Vandalism,
- Rioting, etc.

Determining the threat probability is the goal of the threat analysis. This probability is the frequency with which the threat could or does occur. This information can be obtained through records research, publications, historical data or geographical location, and analysis of the existing environment. To identify threats, interviews should be conducted with personnel knowledgeable in the administrative and procedural areas covering the systems, --- facility managers, local law enforcement, weather bureau officials, etc. Additionally, the history of similar computer centers will assist in threat identification.

E. Identifying Existing Controls

Controls are safeguards which reduce the probability that a threat will exploit a vulnerability to successfully attack an asset. In this case, the team should identify those safeguards that are currently implemented, to determine their effectiveness in reducing the threat probability of successful completion. This information will become important in the analysis phase of the risk assessment, as that is the phase where countermeasure recommendations will be made. This information will aid in determining those countermeasures that could be effective.

8. Data Analysis

The data analysis phase is critical. This is the phase in which all of the collected information will be used to determine what risks the system or application actually face. This risk determination is obtained through analysis of the three areas listed below. The resulting analysis allows management to determine which safeguards should be implemented and which risks should be accepted.

A. Pairing Threats and Vulnerabilities

This phase begins with the process known as threat pairing. For every threat that exists, the vulnerability/vulnerabilities that it would most likely exploit to successfully attack an asset are identified. The following matrix is an example of how this pairing is accomplished.

THREAT	TYPE OF LOSS	VULNERABILITY
Cold / Frost / Snow	Damage / Destruction	Inadequate insulation on pipes
Cold / Frost / Snow	Delay / Denial	Inadequate snow removal
Flood / Water Damage	Damage / Destruction	Inadequate drainage
Blackmail	Disclosure	Inadequate personnel screening

Threat Loss Pairing Example

B. Determining Annual Loss

The next step in the analysis phase is determining the annual loss that could be expected based on the threat and vulnerability pairing. Pairing the threats and frequency of occurrence with the vulnerabilities that the threats can most likely be expected to exploit represents the risk potential associated with the system or application under analysis. To determine the annual loss the threat and vulnerability pairing are matched with one or more asset categories. This matching determines the degree of exposure that the asset may have to an attack.

THREAT	VULNERABILITY	ASSET
Cold / Frost / Snow	Inadequate insulation on pipes	Mail Server
Cold / Frost / Snow	Inadequate insulation on pipes	Client Server
Flood / Water Damage	Inadequate drainage	Mail Server
Flood / Water Damage	Inadequate drainage	Client Server

Asset to Threat/Vulnerability Matching

If the match of these elements were only to occur once, then the asset has a single loss exposure of 1. Once that this matching is completed, the annual loss is be determined. To determine the annual loss that an asset could incur, the single loss exposure is multiplied by the annual frequency at which the threat occurs. This will equal the probable annual loss.

Annual Threat Frequency Calculation Table

Actual Number of Occurrences	**Annual Frequency of Occurrence**
Once a year	1
Twice a year	2
Three times a year	3
Once every 2 years	.5
Once every 5 years	.2
Once every 10 years	.1

If the threat of Flood / Water Damage occurred once every 5 years, the probable annual loss of a Mail Server would be:

1 (Single loss exposure) * .2 (Annual frequency of occurrence) = .2 (probable annual loss of the mail server).

C. Determining Cost-Effective Safeguards

Earlier, we discussed controls in existence and defined what a safeguard was. In this phase of the analysis we will look at:

- The implementation cost of the safeguard,
- The cost to operate the safeguard every year (maintenance & testing), and
- The life cycle of the safeguard.

At the end of this phase of the analysis, the cost benefit analysis should be completed. Start by first assessing the adequacy of the controls, to enhance the security posture of the system or application under review. The basis for assessment of adequacy of current controls will distinguish between controls that are in place and implemented, and controls that are in place and not properly implemented. A resource for recommending improvements to existing or planned controls is the National Computer Security Center’s Evaluated Product List (EPL), which references products that meet specific security criteria. This reference can be located at http://www.radium.ncsc.mil/tpep/.

The criteria for selecting additional controls are:

- The annual cost of the remedial measures shall be less than the reduction in expected loss which they bring about, unless the measure is required by law, regulation, or personnel safety and,
- The mix of security measures shall be the one representing the lowest total cost.

The goal is to present the most cost-effective security control plan, which may also benefit other systems or applications outside the scope of the analysis, --- e.g., any new administrative security procedures will benefit other systems in addition to the system under review. It is critical to recognize and justify the procurement or development of security controls, particularly since some security mechanisms are very expensive and have no obvious benefit. Therefore, the risk analysis effort will help identify instances that are worth the expense of a major security control.

The technical and operational feasibility of a control or combination of controls is as important as the cost considerations. If a security control interferes with system or user productivity, it is less likely to be successfully implemented. For example, in numerous security reviews, security analysts have uncovered instances where password controls have been put in place but circumvented by the users and /or operators, due to the perceived or real inconvenience of remembering and using a password. Also, system audit trails are often voluminous files which occupy valuable disk storage space and take excessive personnel and system resources to review.

9. Reporting Results

The final report is dependant on the audience that is reviewing it. Remember that system administrators, certifying officials, and in some cases the authorizing official may require all of the validated information collected as a result of the analysis. However, management may only require an executive summary, list of recommendations and a cost benefit analysis. It has been found that the simpler a report is to read and understand, the more effective it is. The goal is to be informative, not verbose.

The final report will basically address the following areas:

- Findings,
  - ➢ Threats,
  - ➢ Vulnerabilities, and
  - ➢ Assets
- Recommendations,
  - ➢ Safeguards
  - ➢ Risk Determination,
  - ➢ Cost Benefit Analysis, and
  - ➢ Return on Investment.

For an example of a Risk Assessment Report, please see Appendix A.

APPENDIX A: RISK ASSESSMENT REPORT EXAMPLE

APPENDIX A: RISK ASSESSMENT REPORT EXAMPLE

TBD